HIPAA Information Security Awareness Checklist

1. Summarize the obligation to maintain the security of PHI
   - A. Moral Obligation
   - B. Business Obligation
   - C. Legal Obligation

2. Explain the harm that can occur when proper security measures aren't taken, and give real-life examples.
   - A. Harm to patient
   - B. Harm to organization
   - C. Harm to employee
   - D. Harm to agent or contractor

3. Educate employees, agents, and contractors on the different security risks to your organization, and how to avoid them
   - A. Password maintenance and security
   - B. Other access controls, if used (e.g., access cards/keys, personal identification numbers, biometrics)
   - C. Duty to report all security breaches
   - D. Physical safeguards (e.g., logging off computers, using screensavers, locking doors and files cabinets)
   - E. Email risks
   - F. Computer viruses and other forms of malicious software
   - G. Other security topics/risks

4. Summarize your organization's plan to comply with the HIPAA security regulations.
   - A. Overview of HIPAA compliance plan
   - B. Chief security officer's role
   - C. Policies ad procedures to added/updated
   - D. Hardware/software changes expected
   - E. Security Training Program

5. Say that you will expect cooperation of all employees, agents, and contractors, including the reporting of security violations when they occur.

6. Test employees, agents, and contractors on security.

__Source__: **Many thanks to:**

>>> Samantha Thomas <SThomas@CalSTRS.ca.gov> 08/28/01 01:07PM >>> .... It's a checklist for initial security awareness training sessions developed with the help of health information expert Tom Hanks (whom we've all been reading regularly) for the Health Information Compliance Insider publication. Again, this is the security piece - it assumes that in a separate session the privacy training will be conducted.

Samantha Thomas CISO, CalSTRS (916) 229-4665